

Логика и алгоритмы (весна 2018)

В.Б. Шехтман

20 апреля 2018 г.

Лекция 1

Пропозициональные формулы

Определение 1 Фиксируем счетное множество пропозициональных переменных $PV = \{p_1, p_2, \dots\}$. Множество пропозициональных формул PFm строится из этих переменных, логических связок $\wedge, \vee, \rightarrow, \neg$ и скобок по индукции:

- (1) Если $A \in PV$, то $A \in PFm$.
- (2) Если $A, B \in PFm$, то $(A \wedge B) \in PFm$.
- (3) Если $A, B \in PFm$, то $(A \vee B) \in PFm$.
- (4) Если $A, B \in PFm$, то $(A \rightarrow B) \in PFm$.
- (5) Если $A \in PFm$, то $\neg A \in PFm$.

Таким образом, формулы — это конечные последовательности знаков, т.е. слова в алфавите, состоящем из переменных, связок и скобок. При записи формул применяются дополнительные сокращения: внешние скобки опускаются; для экономии внутренних скобок устанавливается приоритет связок: $\wedge$ сильнее $\vee$, $\vee$ сильнее $\rightarrow$,

Будем использовать знак $\stackrel{\bullet}{=}$ (“графическое равенство”) для обозначения равенства (совпадения) слов.

Лемма 1.1 (Лемма об однозначном анализе формул)

Для любой формулы C выполнено ровно одно из условий:

- (I) $C \in PV$,
- (II) Существует единственная пара формул A, B , такая что $C \stackrel{\bullet}{=} (A \wedge B)$,

(III) Существует единственная пара формул A, B , такая что
 $C \stackrel{\bullet}{=} (A \vee B)$,

(IV) Существует единственная пара формул A, B , такая что
 $C \stackrel{\bullet}{=} (A \rightarrow B)$,

(V) Существует единственная формула A , такая что $C \stackrel{\bullet}{=} \neg A$.

Доказательство этой леммы мы пропустим; его можно найти, например, в [1].

Определение 2 Оценкой (пропозициональных переменных) называется любое отображение $\theta : PV \longrightarrow \{0, 1\}$.

Лемма 1.2 Для любой оценки θ существует единственное отображение $A \mapsto |A|_\theta$ пропозициональных формул в $\{0, 1\}$, такое что для всех A, B

$$(1) \quad |A|_\theta = \theta(A), \text{ если } A \in PV,$$

$$(2) \quad |A \wedge B|_\theta = \min(|A|_\theta, |B|_\theta),$$

$$(3) \quad |A \vee B|_\theta = \max(|A|_\theta, |B|_\theta),$$

$$(4) \quad |A \rightarrow B|_\theta = \max(1 - |A|_\theta, |B|_\theta),$$

$$(5) \quad |\neg A|_\theta = 1 - |A|_\theta.$$

Доказательство Определяем $|C|_\theta$ индукцией по длине C . Если C — переменная, то все ясно: $|C|_\theta = \theta(C)$.

Пусть $n > 1$ и $|C'|_\theta$ однозначно определено на всех формулах C' длины $< n$. Рассмотрим формулу C длины n . По лемме 1.1, возможен ровно один из случаев (2)–(5). В каждом случае $|C|_\theta$ однозначно доопределяется. Например, в случае (2) $C = (A \wedge B)$, и полагаем $|C|_\theta = \min(|A|_\theta, |B|_\theta)$, и т. д. ■

$|C|_\theta$ называется значением формулы C при оценке θ .

Определение 3 Формула называется тавтологией (или общезначимой), если при любой оценке она принимает значение 1.

Формула называется выполнимой, если найдется оценка, при которой она принимает значение 1.

Очевидно, что для любой формулы A :

- A — тавтология $\Leftrightarrow \neg A$ не выполнима.
- A выполнима $\Leftrightarrow \neg A$ — не тавтология.

Определение 4 *Формулы A и B называются равносильными (или эквивалентными), если при всех оценках их значения совпадают.*

Равносильность формул обозначается знаком $\sim$.

Очевидно, что отношение равносильности рефлексивно, симметрично и транзитивно. Обозначим через $\top$ формулу $P_1 \rightarrow P_1$, а через $\perp$ — формулу $P_1 \wedge \neg P_1$.

Лемма 1.3

(1) $A \sim B \Leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$ — тавтология.

(2) A — тавтология $\Leftrightarrow A \sim \top$.

Доказательство (1) Заметим, что

$$|A|_\theta = |B|_\theta \Leftrightarrow |(A \rightarrow B) \wedge (B \rightarrow A)|_\theta = 1.$$

Действительно,

$$|(A \rightarrow B) \wedge (B \rightarrow A)|_\theta = 1 \Leftrightarrow |A \rightarrow B|_\theta = |B \rightarrow A|_\theta = 1$$

Но обе импликации $(A \rightarrow B)$, $(B \rightarrow A)$ истинны только в двух случаях: когда формулы A , B обе истинны или обе ложны, т.е. когда $|A|_\theta = |B|_\theta$.

(2) очевидно. ■

Исчисление высказываний

Тавтологии можно получать как теоремы в некоторой аксиоматической системе — исчислении высказываний. Имеются разные варианты таких исчислений. Мы будем рассматривать исчисление *гильбертовского типа*. Оно задается множеством *аксиом* и *правил вывода*. Теоремы выводятся из аксиом с помощью правил, для этого строится *доказательство* — некоторая последовательность формул.

Приведем одну из формулировок исчисления высказываний (CL).

Схемы аксиом

$$(A1) \quad A \rightarrow (B \rightarrow A)$$

$$(A2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(A3) \quad A \wedge B \rightarrow A$$

$$(A4) \quad A \wedge B \rightarrow A$$

$$(A5) \quad A \rightarrow (B \rightarrow A \wedge B)$$

$$(A6) \quad A \rightarrow A \vee B$$

$$(A7) \quad B \rightarrow A \vee B$$

$$(A8) \quad (A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$$

$$(A9) \quad (A \rightarrow \neg B) \rightarrow ((A \rightarrow B) \rightarrow \neg A)$$

$$(A10) \quad \neg A \rightarrow (A \rightarrow B)$$

$$(A11) \quad \neg A \vee \neg A$$

Здесь A, B, C — произвольные формулы, а потому каждая из схем (A1)–(A11) порождает бесконечную серию аксиом.

Единственное правило вывода — Modus Ponens (MP), которое записывается так:

$$\frac{A, A \rightarrow B}{B}.$$

Эта запись означает, что если доказаны формулы A и $A \rightarrow B$, то можно доказать B .

Определение 5 Доказательство (или вывод) в CL — это конечная последовательность формул, каждая из которых — аксиома или получается из предыдущих по правилу MP.

Точнее: доказательство формулы A — это такая последовательность формул $A_1, \dots, A_n \stackrel{\bullet}{=} A$, что для всех k ($1 \leq k \leq n$)

A_k — аксиома или существуют $i, j < k$, для которых $A_j \stackrel{\bullet}{=} A_i \rightarrow A_k$.

Действительно, из A_i и $A_i \rightarrow A_k$ по MP получается как раз A_k .

Формула A , для которой существует доказательство в CL , называется теоремой CL , или выводимой в CL ; это записывается так: $\vdash_{CL} A$. Индекс CL не пишем, если ясно, что речь идет об этом исчислении.

Пример 1 $\vdash A \vee B \rightarrow B \vee A$.

Приведем доказательство (с комментариями). Для удобства обозначим формулу $B \vee A$ через C .

1. $A \rightarrow C$ (аксиома 7)
2. $B \rightarrow C$ (аксиома 6)
3. $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$ (аксиома 8)
4. $(B \rightarrow C) \rightarrow (A \vee B \rightarrow C)$ (2,4, МР)
5. $A \vee B \rightarrow C$ (1,3, МР)

Формула 5 и есть нужная теорема.

Пример 2 $\vdash A \rightarrow A$. Обозначим эту формулу B .

1. $A \rightarrow B$ (аксиома 1)
2. $A \rightarrow (B \rightarrow A)$ (аксиома 1)
3. $(A \rightarrow (B \rightarrow A)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow A))$ (аксиома 2)
4. $(A \rightarrow B) \rightarrow (A \rightarrow A)$ (2,3, МР)
5. $A \rightarrow A$ (1,4, МР)

Определение 6 Пусть Γ — какое-то множество пропозициональных формул (“гипотез”). Вывод из Γ в CL — это конечная последовательность формул, каждая из которых — аксиома или принадлежит Γ или получается из предыдущих по правилу МР.

Т.е. это последовательность формул $A_1, \dots, A_n$, где для всех k A_k — аксиома или $A_k \in \Gamma$ или существуют $i, j < k$, для которых $A_j \stackrel{\bullet}{=} A_i \rightarrow A_k$.

Формула A выводима из Γ , если существует вывод из Γ с последней формулой A ; обозначение: $\Gamma \vdash_{CL} A$.

Очевидно, что вывод из $\Gamma = \emptyset$ — это обычный вывод из аксиом (в CL).

Лемма 1.4

- (1) Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$.
- (2) Если $\Gamma \vdash A$, то существует конечное $\Delta \subseteq \Gamma$, для которого $\Delta \vdash A$.
- (3) (“транзитивность выводимости”, или “сечение”)
Если $\Gamma \vdash A$, и $\Delta \vdash B$ для всех $B \in \Gamma$, то $\Delta \vdash A$.

Если условие $\Delta \vdash B$ для всех $B \in \Gamma$ обозначить как $\Delta \vdash \Gamma$, то утверждение (3) запишется так:

Если $\Delta \vdash \Gamma$ и $\Gamma \vdash A$, то $\Delta \vdash A$.

Отсюда название “транзитивность”.

Доказательство (1) очевидно.

(2) также очевидно: можно составить Δ из тех гипотез, которые встречаются в выводе A ; их конечное число.

(3) Предположим, что $\Delta \vdash \Gamma$ и $\Gamma \vdash A$. Возьмем вывод A из Γ ; в нем встречаются какие-то гипотезы $B_1, \dots, B_n$ из Γ (возможно, с повторениями):

$\dots B_1, \dots, B_n, \dots, A$.

Заменим в этом выводе каждую B_i на ее вывод Π_i из Δ :

$$\dots \Pi_1, \dots, \Pi_n, \dots, A.$$

Получится вывод A из Δ . Действительно, все формулы из исходного вывода, кроме гипотез B_i , — аксиомы CL или получаются из предыдущих по МР. А в каждом вставном выводе Π_i все формулы — аксиомы CL или входят в Δ или получаются по МР из предыдущих (внутри того же Π_i). ■

Вместо $\{A_1, \dots, A_n\} \vdash_{CL} B$ обычно пишут $A_1, \dots, A_n \vdash_{CL} B$. Говорят также, что $\frac{A_1, \dots, A_n}{B}$ — *производное правило CL* .

Если из выводимости формул $A_1, \dots, A_n$ следует выводимость B , то говорят, что $\frac{A_1, \dots, A_n}{B}$ — *допустимое правило CL* .

Лемма 1.5 *Всякое производное правило CL допустимо.*¹

Доказательство Пусть $\Gamma = \{A_1, \dots, A_n\} \vdash B$. Тогда, если $\emptyset \vdash \Gamma$, то $\emptyset \vdash B$ — по транзитивности выводимости: ■

Транзитивность выводимости означает, что уже доказанные теоремы можно использовать в новых выводах, не повторяя из доказательств. Полученные допустимые правила также можно применять для сокращения доказательств.

Пример 3 Допустимо правило введения конъюнкции

$$\frac{A, B}{A \wedge B}.$$

Действительно, $A, B \vdash A \wedge B$:

1. A (гипотеза)
2. B (гипотеза)
3. $A \rightarrow (B \rightarrow A \wedge B)$ (аксиома А5)
4. $B \rightarrow A \wedge B$ (1,3, МР)
5. $A \wedge B$ (2,4, МР)

Теорема о дедукции для исчисления высказываний

Теорема 1.6 (*теорема² о дедукции*)

$$\Gamma, A \vdash_{CL} B \Leftrightarrow \Gamma \vdash_{CL} A \rightarrow B.$$

Здесь Γ, A обозначает множество $\Gamma \cup \{A\}$.

¹Обратное утверждение тоже верно при некотором уточнении понятия “правило вывода”.

²Конечно, это — не теорема нашего формального исчисления, а утверждение о его свойствах (“метатеорема”).

Доказательство Утверждение $(\Leftarrow)$ почти очевидно. Действительно, пусть $\Gamma \vdash A \rightarrow B$. Тогда имеем $\Gamma, A \vdash A, A \rightarrow B$ и $A, A \rightarrow B \vdash B$ (MP). Отсюда по транзитивности $\Gamma, A \vdash B$.

Утверждение $(\Rightarrow)$ доказывается индукцией по длине вывода B из Γ, A .

(1) Если этот вывод — длины 1, то B — аксиома или гипотеза. Если B — аксиома, то имеем вывод $A \rightarrow B$ (из $\emptyset$):

1. B (аксиома)
2. $B \rightarrow (A \rightarrow B)$ (аксиома A1)
3. $A \rightarrow B$ (1,2, MP)

(2) Если $B \in \Gamma$, то имеем такой же вывод $A \rightarrow B$ из Γ :

1. B (гипотеза)
2. $B \rightarrow (A \rightarrow B)$ (аксиома A1)
3. $A \rightarrow B$ (1,2, MP)

(3) Если $B = A$, то $A \rightarrow B = A \rightarrow A$. Но $\vdash A \rightarrow A$ (пример 2 выше).

(4) Предположим теперь, что $\Gamma, A \vdash B$ и утверждение $(\Rightarrow)$ верно для всех более коротких выводов, т.е.

для всех C , если $\Gamma, A \vdash C$ и вывод C из Γ, A короче, чем вывод B , то $\Gamma \vdash A \rightarrow C$.

Докажем, что $\Gamma \vdash A \rightarrow B$.

Рассмотрим вывод из Γ, A , который заканчивается формулой B . При этом B может оказаться аксиомой или гипотезой (тогда все предыдущие формулы для доказательства B не нужны). Но в этом случае $\Gamma \vdash A \rightarrow B$ по (1)–(3).

Остается случай, когда B получается по MP из формул $C, C \rightarrow B$, причем $\Gamma, A \vdash C$ и $\Gamma, A \vdash C \rightarrow B$ с более короткими доказательствами. По предположению индукции имеем

(*) $\Gamma \vdash A \rightarrow C, A \rightarrow (C \rightarrow B)$.

С другой стороны,

(**) $A \rightarrow C, A \rightarrow (C \rightarrow B) \vdash A \rightarrow B$:

1. $A \rightarrow C$ (гипотеза)
2. $A \rightarrow (C \rightarrow B)$ (гипотеза)
3. $(A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B))$ (аксиома A2)
4. $(A \rightarrow C) \rightarrow (A \rightarrow B)$ (2,3, MP)
5. $A \rightarrow B$ (1,4, MP)

Из (*), (**) по транзитивности получаем $\Gamma \vdash A \rightarrow B$. ■

Отметим частный случай теоремы о дедукции для $\Gamma = \emptyset$:

$$A \vdash B \Leftrightarrow \vdash A \rightarrow B.$$

Пример 4 (правило силлогизма)

$$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C.$$

По теореме дедукции это равносильно

$$A \rightarrow B, B \rightarrow C, A \vdash C.$$

Последнее утверждение очевидно: надо два раза применить MP.

Корректность исчисления высказываний

Теорема 1.7 *Все теоремы CL — тавтологии.*

Доказательство Индукцией по n доказываем что если $\vdash A$ и A имеет вывод длины n , то A — тавтология.

Если A — аксиома, то это проверяется непосредственно.

Шаг индукции.

Пусть A имеет вывод длины n , в котором она получается по МР из B и $B \rightarrow A$. Тогда у этих формул есть выводы длины $< n$, и по предположению индукции, они — тавтологии. Т.е. для любой оценки θ , $|B|_\theta = |B \rightarrow A|_\theta = 1$. А тогда получается, что $|A|_\theta = 1$. Значит, A — тавтология. ■

Следствие 1.8 *CL непротиворечиво, т.е. нет такой формулы A , что $\vdash_{CL} A$ и $\vdash_{CL} \neg A$.*

Доказательство Иначе $A, \neg A$ — тавтологии, и тогда при всех оценках $|A|_\theta = |\neg A|_\theta = 1$, т.е. $|A|_\theta = 1$ и $|A|_\theta = 0$. Это невозможно. ■